Exhibit 37

Excerpts of SW-SEC00151471

From: Pierce, Kellie [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=0150EF14C7A24CB1A0E08EC9FCB06424-PIERCE, KEL]
Sent: 9/18/2019 1:45:24 PM
To: Johnson, Rani [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=0ee57945f15e47b3abaa99a59170ad3f-Johnson, Ra]; Brown, Timothy [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=a1bcd95116e84d6692dd89f9d55c5b7a-Brown, Timo]
Subject: SWICUS: Security Risk Assessment
Attachments: Security Guideline V1.5 and Access Control Self Assessment V1.1_SWICUS 07302019.xlsx

Rani and Tim,
I have been working with Eric and Nelson on the SWICUS self-assessment and want to raise awareness around some of the deficiencies identified:

User Access Management:

- Account Management
  - Local administer rights are not prohibited nor tracked
  - Logical access rights are not disabled if not used w/n 30 days
  - Access is not audited nor monitored
  - No separation of duties related to implemented
  - There is no limit to the number of concurrent sessions for privileged and non-privileged access
  - There is no session lock out timing set

Security Guidelines:

- Endpoint:
  - There is no anti-virus on this system
  - Passwords have no specific parameters, as stated in the IT guidelines
  - Passwords are able to reused and are not changed at a set number of days (i.e. 90 days)
- Systems or Applications:
  - There are is no monitoring or alerts
  - This application is not scanned for vulnerabilities on a monthly basis
- Servers:
  - Unknown license version of the server
  - Server is currently not configured with an enterprise managed anti-virus, anti-malware or hosted firewall
- In House Application:
  - There is no access control and/or domain authentication
- Product Development Requirements:
  - There is no static code analysis performed
  - There is no dynamic vulnerability scanning performed
  - There is no security testing performed
- Auditing & Logging:
  - There is currently no logging or auditing in place

Summary of Security Controls		
%	**#**	**Status**
32%	59	Met
30%	55	Not Applicable N/A
27%	50	Not Met
9%	18	Unknown/Unanswered

	182	Total Number of Controls

Thank you.
Kellie

solarwinds
Kellie Pierce | Security & Compliance Sr. Program Manager | **SolarWinds**
Office: 512.498.6248

DOCUMENT PRODUCED IN NATIVE FORMAT

Security Guidelines (v1.5) and Access Control Guidelines (v1.1) - Self-Assessment

Asset Name:	SWICUS				
Business Unit:	AppMan				
Date Inspected:	2019-08-02				
Document Author:	Fredrik Skogman/Mark Martin				
Security	Security Guideline Section	Sub	Security Requirement	Does the system meet	If the system does not meet the requirement, please provide
Access Control Guidelines V1.1	Account Management	1	The use of shared accounts is prohibited on all information systems. Those systems residing on a guest network are exempt from this requirement	Yes	
Access Control Guidelines V1.1	Account Management	2	Local administrator rights are prohibited. Exceptions must be tracked and additional monitoring must be enabled for all exceptions	No	Local admin is not tracked explicitly
Access Control Guidelines V1.1	Account Management	3	At least two individuals should have administrative accounts to each information system, to provide continuity of operations.	Yes	
Access Control Guidelines V1.1	Account Management	4	Logical access rights should temporarily be disabled when personnel do not need such access for a prolonged period in excess of 30 days.	No	
Access Control Guidelines V1.1	Account Management	5	Supervisors, Human Resources, and the System Administrator shall be notified in a timely manner about termination, transfer of employees and contractors with access rights to internal information systems and data.	Yes	
Access Control Guidelines V1.1	Account Management	6	Access should be promptly removed when no longer required.	Yes	
Access Control Guidelines V1.1	Account Management	7	Any changes to access level authorizations must be monitored and validated by the security operations team or appropriate delegates	Yes	
Access Control Guidelines V1.1	Account Management	8	Secure delivery of access credentials is required.	Yes	
Access Control Guidelines V1.1	Access Enforcement	1	Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities	Yes	
Access Control Guidelines V1.1	Access Enforcement	2	Default passwords for all information systems with data classified as moderate or high must be reset and checked via vulnerability scanners	N/A	There are no default passowords
Access Control Guidelines V1.1	Access Enforcement	3	All access must be audited and monitored	No	See above on local admin usage
Access Control Guidelines V1.1	Access Enforcement	4	For all information systems with data classified as low require a username and password	Yes	
Access Control Guidelines V1.1	Access Enforcement	5	For all information systems with data classified as moderate or high require strong authentication including risk based authentication or multi-factor	Yes	Only a list of specific users have access to VPN on which system reside,
Access Control Guidelines V1.1	Information Flow Enforcement	1	Systems shall enforce data flow controls using security attributes on information, source, and destination objects as a basis for flow control decisions	N/A	
Access Control Guidelines V1.1	Information Flow Enforcement	2	A Data map must exist showing data flows for sensitive data for all information systems with data classified as moderate or high	Yes	
Access Control Guidelines V1.1	Information Flow Enforcement	3	The security of the sender the receiver and the transport must be audited and monitored	Yes	
Access Control Guidelines V1.1	Separation of Duties	1	Duties of individuals shall be separated as necessary, to prevent malevolent activity without collusion.		
Access Control Guidelines V1.1	Separation of Duties	2	These duties must be documented and implemented through assigned information systems access authorizations		
Access Control Guidelines V1.1	Separation of Duties	3	Separation of duties must be implemented such that critical/operational information system functions are separated into distinct jobs to prevent a single	No	
Access Control Guidelines V1.1	Least Privilege	1	Users of information system accounts, or roles, with access to administrative accounts are required to use non-privileged accounts or roles, when accessing	N/A	
Access Control Guidelines V1.1	Least Privilege	2	Security functions and configuration of security controls are limited to personnel in the Security team or approved delegates.	Yes	
Access Control Guidelines V1.1	Least Privilege	3	System Administrators must have both an administrative account and at least one non-privileged user account. Administrators must use their administrative	Yes	
Access Control Guidelines V1.1	Least Privilege	4	Authorization to use super user accounts on the information system is limited to designated system administration personnel	Yes	
Access Control Guidelines V1.1	Least Privilege	5	Privilege levels for code execution – Information systems should execute at the same level of the users executing the software	Yes	
Access Control Guidelines V1.1	Least Privilege	6	All privileged access must be monitored and audited on a regular basis	Yes	
Access Control Guidelines V1.1	Unsuccessful Login Attempts	1	A maximum of 5 invalid authentication attempts shall automatically lock the account for a minimum of a 15-minute period when the maximum number of	Yes	
Access Control Guidelines V1.1	System User Notification	1	Information systems shall display an approved system use notification message or banner before granting access to the system that provides privacy and	N/A	
Access Control Guidelines V1.1	Concurrent Session Control	1	The information system should limit the number of concurrent sessions for privileged and non-privileged access. For privileged access, the number of	No	
Access Control Guidelines V1.1	Session Lock	1	Information systems should prevent further access to the system or application by initiating a session lock after a 15-minute period inactivity or upon receiving	No	
Access Control Guidelines V1.1	Remote Access	1	SolarWinds VPN gateways will be configured and managed by the Information Technology department	Yes	
Access Control Guidelines V1.1	Remote Access	2	VPN Client must validate the integrity of the client device prior to connection		
Access Control Guidelines V1.1	Remote Access	3	VPN users will be automatically disconnected from the corporate network after a defined period of inactivity		
Access Control Guidelines V1.1	Remote Access	4	The VPN gateway is limited to an absolute connection time of 24 hours		
Access Control Guidelines V1.1	Remote Access	5	Access to public facing corporate applications must utilize the access enforcement guidelines as outlined above		
Access Control Guidelines V1.1	Wireless Access	1	Client devices connecting to the WLAN must utilize two-factor authentication (i.e., digital certificates);	N/A	System is placed in an isolated network only accessible via VPN
Access Control Guidelines V1.1	Wireless Access	2	WLAN infrastructure must authenticate each client device prior to permitting access to the WLAN	N/A	
Access Control Guidelines V1.1	Wireless Access	3	LAN user authorization infrastructure (i.e., Active Directory) must be used to authorize access to LAN resources;	N/A	
Access Control Guidelines V1.1	Wireless Access	4	Only corporate owned or leased equipment shall be granted access to an internal WLAN;	N/A	
Access Control Guidelines V1.1	Wireless Access	5	All WLAN communications must utilize a secure encryption algorithm	N/A	
Access Control Guidelines V1.1	Wireless Access	6	Physical or logical separation between WLAN and wired LAN segments must exist;	N/A	
Access Control Guidelines V1.1	Wireless Access	7	All corporate WLAN access and traffic is monitored for malicious activity	N/A	
Access Control Guidelines V1.1	Use of External Information Systems	1	Has approved information system connection or processing agreements with the organizational entity		
Access Control Guidelines V1.1	Use of External Information Systems	2	Has verified the implementation of required security controls on the external system as specified in information security guidelines		
Security Guidelines V1.5	Endpoints	1.1	Endpoint Encryption enabled and managed – Bitlocker is the company standard, alternatives are acceptable if managed and audited	Yes	
Security Guidelines V1.5	Endpoints	1.2	Anti-virus – Symantec Endpoint Protection is the managed and audited company standard	No	
Security Guidelines V1.5	Endpoints	1.3	Automated patch deployment – Patches updates and monitoring are required	Yes	
Security Guidelines V1.5	Endpoints	1.4	Domain Authentication – Required in most cases exemptions granted on a case by case basis	No	See above on certs
Security Guidelines V1.5	Endpoints	1.5	The password requirements listed below can be met if Microsoft Active Directory domain authentication is used as the means of identifying authorized users.	N/A	
Security Guidelines V1.5	Endpoints	1.5.1	Passwords cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters	No	
Security Guidelines V1.5	Endpoints	1.5.1.1	Passwords must be at least 8 characters in length.	Yes	
Security Guidelines V1.5	Endpoints	1.5.1.2	Passwords must contain characters from three of the following four categories:	No	
Security Guidelines V1.5	Endpoints	1.5.1.3	English uppercase characters (A through Z).	No	
Security Guidelines V1.5	Endpoints	1.5.1.4	English lowercase characters (a through z).	No	
Security Guidelines V1.5	Endpoints	1.5.1.5	Base 10 digits (0 through 9).	No	
Security Guidelines V1.5	Endpoints	1.5.1.6	Non-alphabetic characters (for example, !, $, #, %).	No	
Security Guidelines V1.5	Endpoints	1.5.2	Passwords are saved only as one way hashed, encrypted files. Access to password files is restricted only to system administrators. If the authentication	Yes	
Security Guidelines V1.5	Endpoints	1.5.3	Password history: users should not be able to re-use the last five (5) passwords	No	
Security Guidelines V1.5	Endpoints	1.5.4	Password age: Passwords must be changed every 90 days		
Security Guidelines V1.5	Endpoints	1.5.5	User credentials must be communicated in a secure manner. Passwords must be shared through a different distribution channel than the one used for the	Yes	
Security Guidelines V1.5	Endpoints	1.6	Data Loss Prevention (DLP) Enabled – Required in most cases exemptions granted on a case by case basis	Yes	
Security Guidelines V1.5	Endpoints	1.7	IT managed and audited	No	AppMan SRE team owns and manages this system
Security Guidelines V1.5	Endpoints	1.8	Process to disable access and wipe data must be in place	Yes	
Security Guidelines V1.5	Endpoints	1.9	Minimal control must be given to helpdesk and others	Yes	
Security Guidelines V1.5	Mobile Devices	2.1	Encryption enabled	Yes	
Security Guidelines V1.5	Mobile Devices	2.2	Authentication required	Yes	
Security Guidelines V1.5	Mobile Devices	2.3	Managed (Optional)	N/A	
Security Guidelines V1.5	Networks	3.1	Data classified as moderate or higher must flow over encrypted channels (i.e. HTTPs/ TLS 1.1 or greater). Exceptions will be reviewed on a case by case basis.	Yes	
Security Guidelines V1.5	Networks	3.2	Network devices vulnerability scan completed monthly	N/A	Deployed in AWS
Security Guidelines V1.5	Networks	3.3	Network devices patched quarterly (Depending on level of vulnerability)	N/A	
Security Guidelines V1.5	Networks	3.4	Minimal Essential Access model enabled. Segmentation/isolation models must be utilized to isolate and contain the environment	Yes	
Security Guidelines V1.5	Networks	3.5	Daily monitoring of all network security logs. Immediate alerts enabled for all critical issues	N/A	
Security Guidelines V1.5	Networks	3.6	Network scanning to include IDS/Network Malware Detection/ URL filtering and Sandbox support for unknown risks	N/A	
Security Guidelines V1.5	Networks	3.7	The password requirements listed below can be met if Microsoft Active Directory domain authentication is used as the means of identifying authorized users.	N/A	
		3.7.1	Passwords cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters	N/A	
Security Guidelines V1.5	Networks	3.7.1.1	Passwords must be at least 8 characters in length.	N/A	
Security Guidelines V1.5	Networks	3.7.1.2	Passwords must contain characters from three of the following four categories:	N/A	
Security Guidelines V1.5	Networks	3.7.1.3	English uppercase characters (A through Z).	N/A	
Security Guidelines V1.5	Networks	3.7.1.4	English lowercase characters (a through z).	N/A	
Security Guidelines V1.5	Networks	3.7.1.5	Base 10 digits (0 through 9).	N/A	
Security Guidelines V1.5	Networks	3.7.1.6	Non-alphabetic characters (for example, !, $, #, %).	N/A	
Security Guidelines V1.5	Networks	3.7.2	Passwords are saved only as one way hashed, encrypted files. Access to password files is restricted only to system administrators. If the authentication	N/A	
Security Guidelines V1.5	Networks	3.7.3	Password history: users should not be able to re-use the last five (5) passwords	N/A	
Security Guidelines V1.5	Networks	3.7.4	Password age: Passwords must be changed every 90 days.	N/A	

Security Guidelines V1.5	Networks	3.7.5	User credentials must be communicated in a secure manner. Passwords must be shared through a different distribution channel than the one used for the	N/A	
Security Guidelines V1.5	Networks	3.11	Network components required to be under IT Audit and IT management	N/A	
Security Guidelines V1.5	Networks	3.12	Network audit should show no clear text or data classified as moderate or higher	N/A	
Security Guidelines V1.5	Systems or Applications	4.1	Monthly IT Managed Vulnerability Scans	No	
Security Guidelines V1.5	Systems or Applications	4.2	Quarterly patching schedule for all vulnerabilities and accelerated program for critical vulnerabilities	Yes	
Security Guidelines V1.5	Systems or Applications	4.3	Daily IT monitoring and real time alerting for critical issues	No	
Security Guidelines V1.5	Systems or Applications	4.4	Hardened and all extraneous services disabled	Yes	
Security Guidelines V1.5	Systems or Applications	4.5	Adherence to standard defined system build and configuration	Yes	
		4.6	The password requirements listed below can be met if Microsoft Active Directory domain authentication is used as the means of identifying authorized users.		
Security Guidelines V1.5	Systems or Applications	4.6.1	Passwords cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters	No	
Security Guidelines V1.5	Systems or Applications	4.6.1.1	Passwords must be at least 8 characters in length.	Yes	
Security Guidelines V1.5	Systems or Applications	4.6.1.2	Passwords must contain characters from three of the following four categories:		
Security Guidelines V1.5	Systems or Applications	4.6.1.3	English uppercase characters (A through Z).	No	
Security Guidelines V1.5	Systems or Applications	4.6.1.4	English lowercase characters (a through z).	No	
Security Guidelines V1.5	Systems or Applications	4.6.1.5	Base 10 digits (0 through 9).	No	
Security Guidelines V1.5	Systems or Applications	4.6.1.6	Non-alphabetic characters (for example, !, $, #, %).	No	
Security Guidelines V1.5	Systems or Applications	4.6.2	Passwords are saved only as one way hashed, encrypted files. Access to password files is restricted only to system administrators. If the authentication	Yes	
Security Guidelines V1.5	Systems or Applications	4.6.3	Password history: users should not be able to re-use the last five (5) passwords	No	
		4.6.4	Password age: Passwords must be changed every 90 days.	No	
Security Guidelines V1.5	Systems or Applications	4.6.5	User credentials must be communicated in a secure manner. Passwords must be shared through a different distribution channel than the one used for the	N/A	
Security Guidelines V1.5	Systems or Applications	4.7	Local privileged accounts disabled and access and usage of privileged accounts audited and monitorec	No	
Security Guidelines V1.5	Systems or Applications	4.8	Privileged account access requires greater than username/pw access (multi-factor authentication	Yes	
Security Guidelines V1.5	Server Hardening	5.1	Server operating systems must be an official SolarWinds licensed and supported version	Unsure	
Security Guidelines V1.5	Server Hardening	5.2	Appropriate vendor supplied security patches and firmware updates must be applied	Yes	
Security Guidelines V1.5	Server Hardening	5.3	Unnecessary software, system services, protocols, ports, and drivers must be removed	Yes	
Security Guidelines V1.5	Server Hardening	5.4	Servers must be configured with enterprise managed anti-virus, anti-malware software, and a host based firewall. Exceptions shall be granted on a case by	No	
Security Guidelines V1.5	Server Hardening	5.5	Local system accounts and credentials should not be used. The default administrator account should be renamed. Guest accounts should be renamed and	N/A	
Security Guidelines V1.5	Server Hardening	5.6	Appropriate local file system/sharing permissions, local/physical security, reporting, intrusion detection, and logging/auditing must be enabled.		
Security Guidelines V1.5	Server Hardening	5.7	Appropriate Domain-based Active Directory server based group policies must be enforced. Exceptions shall be granted on a case by case basis	N/A	
Security Guidelines V1.5	Server Hardening	5.8	Post-Install operating system, utility/system service patches, database, web, and application security patches shall be pre-tested and deployed on a regular	N/A	Mostly run via AWS manages services
Security Guidelines V1.5	Server Hardening	5.9	Periodic audits of server compliance shall be conducted at least annually. Results shall be documented and any deficiencies corrected.	Yes	
Security Guidelines V1.5	In House Applications	6.1	Access Control and Domain authentication.	No	
Security Guidelines V1.5	In House Applications	6.2	Privileged access controlled especially for databases/data stores	Yes	
Security Guidelines V1.5	In House Applications	6.3	IT audit and monitoring enabled.	No	
Security Guidelines V1.5	In House Applications	6.4	Data classified as moderate or higher should be encrypted or anonymized if possible	Yes	
Security Guidelines V1.5	In House Applications	6.5	If unable to encrypt or anonymize data, a need to know model should be enabled and increased audit frequency and inspection of access should be completed	Yes	
Security Guidelines V1.5	In House Applications	6.6	The password requirements listed below can be met if Microsoft Active Directory domain authentication is used as the means of identifying authorized users.	No	
Security Guidelines V1.5	In House Applications	6.6.1	Passwords cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters	No	
Security Guidelines V1.5	In House Applications	6.6.1.1	Passwords must be at least 8 characters in length.	Yes	
Security Guidelines V1.5	In House Applications	6.6.1.2	Passwords must contain characters from three of the following four categories:	No	
Security Guidelines V1.5	In House Applications	6.6.1.3	English uppercase characters (A through Z).	No	
Security Guidelines V1.5	In House Applications	6.6.1.4	English lowercase characters (a through z).	No	
Security Guidelines V1.5	In House Applications	6.6.1.5	Base 10 digits (0 through 9).	No	
Security Guidelines V1.5	In House Applications	6.6.1.6	Non-alphabetic characters (for example, !, $, #, %).	No	
Security Guidelines V1.5	In House Applications	6.6.2	Passwords are saved only as one way hashed, encrypted files. Access to password files is restricted only to system administrators. If the authentication	Yes	
Security Guidelines V1.5	In House Applications	6.6.3	Password history: users should not be able to re-use the last five (5) passwords	No	
Security Guidelines V1.5	In House Applications	6.6.4	Password age: Passwords must be changed every 90 days.	No	
Security Guidelines V1.5	In House Applications	6.6.5	User credentials must be communicated in a secure manner. Passwords must be shared through a different distribution channel than the one used for the	Yes	
Security Guidelines V1.5	In House Applications	6.7	Applications should be scanned quarterly for vulnerabilities	No	
Security Guidelines V1.5	In House Applications	6.8	Applications should be patched quarterly with more attention given to critical vulnerabilities	Yes	
Security Guidelines V1.5	In House Applications	6.9	For data stores – Encryption should be enabled if possible. Obfuscation via anonymization if not. If clear text storage – Increased authentication, access	Yes	
Security Guidelines V1.5	3rd Party Applications	7.1	Third party applications that access, manage, or store data classified as moderate or higher, are expected to provide a security policy, privacy policy, data	N/A	No access from third party systems
Security Guidelines V1.5	3rd Party Applications	7.2	An assessment of their security policy should be performed by the IT Security team and an annual audit of their controls should be performed	N/A	
Security Guidelines V1.5	3rd Party Applications	7.3	The password requirements listed below can be met if Microsoft Active Directory domain authentication is used as the means of identifying authorized users.	N/A	
Security Guidelines V1.5	3rd Party Applications	7.3.1	Passwords cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters	N/A	
Security Guidelines V1.5	3rd Party Applications	7.3.1.1	Passwords must be at least 8 characters in length.	N/A	
Security Guidelines V1.5	3rd Party Applications	7.3.1.2	Passwords must contain characters from three of the following four categories:	N/A	
Security Guidelines V1.5	3rd Party Applications	7.3.1.3	English uppercase characters (A through Z).	N/A	
Security Guidelines V1.5	3rd Party Applications	7.3.1.4	English lowercase characters (a through z).	N/A	
Security Guidelines V1.5	3rd Party Applications	7.3.1.5	Base 10 digits (0 through 9).	N/A	
Security Guidelines V1.5	3rd Party Applications	7.3.1.6	Non-alphabetic characters (for example, !, $, #, %).	N/A	
Security Guidelines V1.5	3rd Party Applications	7.3.2	Passwords are saved only as one way hashed, encrypted files. Access to password files is restricted only to system administrators. If the authentication	N/A	
Security Guidelines V1.5	3rd Party Applications	7.3.3	Password history: users should not be able to re-use the last five (5) passwords	N/A	
Security Guidelines V1.5	3rd Party Applications	7.3.4	Password age: Passwords must be changed every 90 days.	N/A	
Security Guidelines V1.5	3rd Party Applications	7.3.5	User credentials must be communicated in a secure manner. Passwords must be shared through a different distribution channel than the one used for the	N/A	
Security Guidelines V1.5	3rd Party Applications	7.4	Where possible monitoring and auditing of 3rd party applications should be conducted in a similar form to in house applications and the 3rd party vendor	N/A	
Security Guidelines V1.5	3rd Party Applications	7.5	Secure Delete: 3rd Party; if an application is hosted by a 3rd party, the 3rd party must delete and demonstration that the data has been deleted. For any 3rd	N/A	
Security Guidelines V1.5	Environment	8.1	The components of the environment should be known and audited and reported on independenth	N/A	Mostly based on AWS manages services
Security Guidelines V1.5	Environment	8.2	The overall design of the environment should promote containment of incidents and limit exposure	Yes	
Security Guidelines V1.5	Environment	8.3	The environment should be tested yearly with a focus on incident response and management	Need to ask Security team	
Security Guidelines V1.5	Product Development Requirements	9.1	Continuous Training: Security training is required. In order to execute to a high level of secure development, teams must be educated on the best practices and	No	
Security Guidelines V1.5	Product Development Requirements	9.2	Requirements Analysis: Requirements are analyzed and considered to expose any security and privacy constraints that must be designed into the system. Features are evaluated to determine what potential threats and vulnerabilities implementation may introduce to the software. Security artifacts are created to track the design of these features and ensure that security principles are applied. Focus is given to identification of features that include security aspects such a authentication, access control, encryption and cryptographic algorithms, credential management and securing private data. Each identified area is then translated into security requirements that are validated at specific gates during the development lifecycle	Yes	
Security Guidelines V1.5	Product Development Requirements	9.3	Secure Development	Yes	
		9.3.1	Secure Design: Secure design means understanding the threat landscape, attack surface and taking a Security by design approacl	Yes	
Security Guidelines V1.5	Product Development Requirements	9.3.1.1	Threat Modeling: Threat modeling should be used to understand areas of risk so that developers and architects can apply secure design principles that follow	Yes	
Security Guidelines V1.5	Product Development Requirements	9.3.1.2	Attack Surface Reduction: Attack surface reduction exercises should be used to evaluate potential areas of vulnerability and focus on reducing the total	Yes	
Security Guidelines V1.5	Product Development Requirements	9.3.1.3	Vulnerability Scanning: All third-party and open source components planned for use in a design should be scanned for vulnerabilities to ensure that SolarWinds	Yes	
Security Guidelines V1.5	Product Development Requirements	9.3.2	Secure Coding - As coding begins, teams leverage industry best practices guidelines for secure coding. These guidelines are coupled with code reviews anc	Yes	
Security Guidelines V1.5	Product Development Requirements	9.4	Security Testing		
Security Guidelines V1.5	Product Development Requirements	9.4.1	Static Analysis: Static code analyzers are used for detecting security vulnerabilities in a developer's code. Analyzers are deployed for products and are used as coding continues. These tools provide near real-time feedback on potential security issues as developers are writing code. Development teams are expected to review and prioritize any warnings that are generated. Continuous scanning allows for quick verification any reported issue.	No	
Security Guidelines V1.5	Product Development Requirements	9.4.2	Dynamic Analysis: Engineering's software development test framework includes a collection of automated and manual testing tools, such as penetration and vulnerability scanning tools, which are used to verify the integrity and security of the software product while deployed. These tools look for known vulnerabilities, security defects and incorporate requirements that were derived from the security analysis that occurred during the planning phase. Dynamic testing in conjunction with static code analysis are continuous activities that recur throughout the development process	No	
Security Guidelines V1.5	Product Development Requirements	9.5	Security Testing: Prior to release, the Final Security Review (FSR) assesses the complete security posture of the software system. The review will ensure that all	No	
Security Guidelines V1.5	Product Development Requirements	9.6	Release : Prior to release, the Final Security Review (FSR) assesses the complete security posture of the software system. The review will ensure that all prior	No	
Security Guidelines V1.5	Product Development Requirements	9.7	Response: SolarWinds recognizes that even with the application of a robust SDL that will prevent known vulnerabilities from exiting in a released product, over	Yes	

Security Guidelines V1.5	Auditing and Logging	10.1	All systems that handle GDPR data must log and audit all access, administrative changes, server events related to the application, system, and security events.	No (work in progress)	
Security Guidelines V1.5	Auditing and Logging	10.2	Security audit logs must be sent to a centrally managed and monitored security information and event management system (SIEM) in order to provide real-	No	
Security Guidelines V1.5	Auditing and Logging	10.3	The auditing and logging requirements listed below can be met if the security audit logs are being sent to a centrally managed and monitored SIEM. Otherwise,		
Security Guidelines V1.5	Auditing and Logging	10.4	Security audit logs must be retained for a minimum of 60 days or as needed for business purposes.	No	
Security Guidelines V1.5	Auditing and Logging	10.5	Security audit logs must be integrated into an audit review process that supports investigation and response to suspicious user activities and to identify	No	
Security Guidelines V1.5	Auditing and Logging	10.6	Access to security audit logs must be limited to authorized users	No	
Security Guidelines V1.5	Auditing and Logging	10.7	Separation of duties must be enforced to ensure the integrity of the log data	No	
Security Guidelines V1.5	Secure Delete	11.1	For third party providers contract language or public policies must be in place to support:	Yes	
Security Guidelines V1.5	Secure Delete	11.1.1	The deletion of GDPR data upon request and the attestation of the deletion	Yes	
Security Guidelines V1.5	Secure Delete	11.1.2	A documented storage device decommissioning process	N/A	Located in AWS
Security Guidelines V1.5	Secure Delete	11.1.3	Exceptions shall be granted on a case by case basis		
Security Guidelines V1.5	Secure Delete	11.2	For in-house systems and applications that store data classified as moderate:		
Security Guidelines V1.5	Secure Delete	11.2.1	Must support deletion. Soft delete or marked for deletion is acceptable as long as the device remains managed and is performing the same function.	Yes	
Security Guidelines V1.5	Secure Delete	11.2.2	If the device is repurposed or is no longer managed it must be formatted, reinitialized and all data hard deleted.	N/A	Located in AWS
Security Guidelines V1.5	Secure Delete	11.3	When a device has reached the end of its useful life. The device must be decommissioned/destroyed following the techniques detailed in the most recent NIST	N/A	Located in AWS